

California Home

Wednesday, November 19, 2003

[HHSDC Home](#)[BP Home Page](#)[The MSC](#)[CMM](#)[POST Enterprise](#)[The Project Office](#)[Life Cycle Processes](#)[Search BP](#)[HHSDC Links](#)[Resources Library](#)[QAWG](#) **NEW!**[SID Policy](#) **NEW!**[Contact Us](#)

☒ My CA

Risk Management Supporting Process

The purpose of risk management is to identify threats to project success and to mitigate or eliminate negative impacts to the project. Not all risks can be eliminated, but mitigation and contingency plans can be developed to lessen their impact if they occur.

The basic elements of the [Risk Management Process](#) are:

- **[Risk Identification](#)** - Risk identification consists of determining which risks are likely to affect the project and documenting the characteristics of each. Risk identification is not a one-time event; it should be performed on a regular basis throughout the project. Risk identification should address both internal and external risks. Internal risks are things that the project team can control or influence; external risks are things beyond the control or influence of the project team.
- **[Risk Analysis](#)** - Risk analysis involves evaluating risks and risk interactions to assess the range of possible project outcomes. It is primarily concerned with determining which risk events warrant response.
- **[Risk Planning \(Mitigation and Contingency Planning\)](#)** - Risk planning is composed of two parts: mitigation planning and contingency planning. It involves assigning responsibility for risk actions, developing mitigation and/or contingency plans, developing measurements and developing action plans to respond to the risk. Note that it may not always be possible or feasible to mitigate risks; some risks may have to be accepted.
- **[Risk Implementation](#)** - Risk implementation involves the implementation of the risk mitigation and contingency plans developed in the previous step.
- **[Risk Tracking & Control](#)** - Risk Tracking & Control follows the progress of the risk and its probability, as well as the status of any mitigation strategies that have been executed. When changes occur, the basic cycle of identify, analyze, and respond is repeated.
- **[Communication](#)** - Effective communication helps to ensure risks are identified and tracked throughout all levels of the project.

At the beginning of the project, the Project Office should identify the approach to managing risk in the [Risk Management Plan](#), including a [risk management process](#) and recommended [features of a risk management system](#). When the contractor begins work, they should also deliver a Risk Management Plan describing how they will manage risks within their organization.

References:

- [SID's Policy for Risk Management](#) (pdf)
- [SID's CMM Standards for Risk Management](#) (pdf)
- DOF TOSU Budget Letter 03-04, IT Oversight Framework, Section 5 ([MS Word](#) or [PDF](#))
- [IEEE 1540- 2001](#), Standard for Risk Management (link to pdf)
- [IEEE 1490-1998, Adoption of PMI's PMBOK, Section 11 Risk Management](#) (pdf)
- [SEI's SA-CMM](#), Key Process Area 3.4 (pdf)
- [SEI's Taxonomy-Based Risk Identification](#) (pdf)
- [SEI's Software Risk Evaluation \(SRE\) Method Description](#) (pdf)
- [SPMN's Risk Radar User Manual](#) (pdf)
- [EBT Risk Identification Form](#) (MS Word)

California Home

Wednesday, November 19, 2003



[HHSDC Home](#)

[BP Home Page](#)

[The MSC](#)

[CMM](#)

[POST Enterprise](#)

[The Project Office](#)

[Life Cycle Processes](#)

[Search BP](#)

[HHSDC Links](#)

[Resources Library](#)

[QAWG **NEW!**](#)

[SID Policy **NEW!**](#)

[Contact Us](#)



SID follows the SEI risk management process as shown in the diagram below.

☒ My CA

Risk Management Process Diagram

[Risk Main](#)




[HHSDC Home](#)
[BP Home Page](#)
[The MSC](#)
[CMM](#)
[POST Enterprise](#)
[The Project Office](#)
[Life Cycle Processes](#)
[Search BP](#)
[HHSDC Links](#)
[Resources Library](#)
[QAWG NEW!](#)
[SID Policy NEW!](#)
[Contact Us](#)


☒ My CA

Risk Identification

[Risk Main](#)

Risks can come from a variety of sources, both internal and external to the project. The Project Office must also consider political and organizational risks. Although the Project Office cannot always eliminate these risks, effective communication can mitigate some of the impacts in these critical areas.

The first step in managing risks is to identify them. Risk identification should consider all areas of a project and both internal and external factors. Potential risks and their causes should be identified and documented. Risks should be identified through the use of a questionnaire (such as [SEI's Taxonomy-based Questionnaire](#) (pdf)) and interviews with project management, staff, stakeholders and users.

Often the IV&V Vendor will perform a risk assessment as one of their first tasks to help focus and refine their oversight efforts. Risk identification should be an on-going task throughout the project life cycle.

Some common risks to software projects are [Boehm, 1989]:

- Continuous stream of requirements changes
- Personnel shortfalls
- Unrealistic schedules and budgets
- Developing the wrong software functions
- Developing the wrong user interface
- "Goldplating" - paying too much attention to what the customer wants changed
- Shortfalls in external furnished components
- Real-time performance shortfalls

Risks which are unique to the State include:

- Employing technologies new to the State
- Changing political climate
- Federal and State legislation imposing requirements
- Insufficient staffing or budget to adequately manage the project

There may be specific risks associated with a particular phase also, such as in implementation and [Maintenance and Operations \(M&O\)](#)

Samples:

- [Risk Tracking Form](#) (MS Word)
- [EBT Risk Identification Form](#) (MS Word)

California Home

Wednesday, November 19, 2003

[HHSDC Home](#)[BP Home Page](#)[The MSC](#)[CMM](#)[POST Enterprise](#)[The Project Office](#)[Life Cycle Processes](#)[Search BP](#)[HHSDC Links](#)[Resources Library](#)[QAWG](#) **NEW!**[SID Policy](#) **NEW!**[Contact Us](#)

search

☒ My CA[Risk Main](#)

Risk Analysis

Risk analysis & prioritization considers each risk and its cause to determine:

- Classification of the risk (for instance, according to the SEI Taxonomy)
- Impacts of the risk occurrence
- Probability of its occurrence
- Timeframe when the risk will likely occur
- Risk exposure (based on the impact and probability)
- Risk severity/Priority given other current risks
- Risk escalation (based on severity and project criticality)
- Level of control (ability to influence the risk status)
- Mitigation and contingency strategies and options

During the risk analysis, each risk should be prioritized based on its impact and probability of occurrence (exposure level). Prioritization helps the Project Manager to focus efforts and resources on the most critical risks. The [SID Policy for Risk Management](#) describes the definitions and criteria for each of the factors above.

Based on the risk descriptors above, the project must decide how to approach the identified risks. Generally, a mitigation and/or contingency plan will be developed to address the risk. The project must prioritize the risk planning efforts given the available resources, and exposure and severity of the risks.

Some risks may be beyond the control or mitigation of the Project Office. These are typically political or legislative issues. In these cases, communication and contingency planning may be the only cost-effective and feasible responses to the risk (accept the risk is likely).

California Home

Wednesday, November 19, 2003

[HHSDC Home](#)[BP Home Page](#)[The MSC](#)[CMM](#)[POST Enterprise](#)[The Project Office](#)[Life Cycle Processes](#)[Search BP](#)[HHSDC Links](#)[Resources Library](#)[QAWG](#) **NEW!**[SID Policy](#) **NEW!**[Contact Us](#)

☒ My CA

Risk Planning (Mitigation and Contingency Plans)

[Risk Main](#)

The risk planning step involves developing mitigation and contingency plans, as appropriate, to address a specific risk. The risk owner is responsible for developing these plans and ensuring they are implemented as planned. Tracking measures should also be developed. Objective measurements are preferred, but in some cases only subjective measurements may be available.

Mitigation Plans:

Mitigation strategies try to identify ways to minimize or eliminate project risks. Depending on the severity of the risk and the level of effort of the mitigation strategies, it may be appropriate to initiate several mitigation activities. It is important, however, to balance the exposure of the risk with the cost-effectiveness of the mitigation strategy and the likelihood of the desired effect.

If the mitigation activities will not be executed immediately, it is important to identify a trigger event or measurement which will initiate the mitigation activities. Tracking measurements should also be developed to provide a way to track the status and effectiveness of the risk actions.

The following information should be documented in a mitigation plan:

- The risk to be mitigated
- Selected mitigation strategies to be implemented
- When each mitigation activity will commence (trigger event)
- How and when (frequency of) the mitigation activities will be tracked (measures)
- Specific mitigation actions to be implemented
- Who is responsible for the mitigation activities
- Who is responsible for tracking mitigation effectiveness

Contingency Plans:

For those risks where it is unlikely or uncertain that the mitigation will be effective, a contingency plan should be developed. Contingency plans attempt to minimize the effects of the risk assuming the event does occur (also known as "damage control").

A trigger mechanism should be identified that indicates when the contingency plan should be initiated. In some cases, the plan may be initiated before the risk occurs or in parallel with the mitigation activities in order to be prepared for the risk occurrence.

Typical components of a contingency plan include:

- Description of the impending risk
- Anticipated effects on project staff, users, stakeholders
- Anticipated effects on project schedule
- Anticipated effects on project budget
- Anticipated effects on work products or deliverables
- Desired outcome of contingency activities
- Communication strategy as risk becomes more likely
- What activities will be executed to minimize risk's effects
- Who is responsible for the activities
- When will the activities occur (what is the trigger event)
- How to evaluate and track the effect of the contingency activities
- When the contingency activities will cease (by a certain date or when a specific desired effect has occurred)

Outline:

- [Mitigation Plan Outline](#) (MS Word)

California Home

Wednesday, November 19, 2003

[HHSDC Home](#)[BP Home Page](#)[The MSC](#)[CMM](#)[POST Enterprise](#)[The Project Office](#)[Life Cycle Processes](#)[Search BP](#)[HHSDC Links](#)[Resources Library](#)[QAWG](#) **NEW!**[SID Policy](#) **NEW!**[Contact Us](#)

search

☒ My CA

Risk Implementation

Risk Main

Risk implementation is the performance of the activities described by the risk mitigation and contingency plans. The appropriate measures and status are reported to track effectiveness. If there are significant changes in status or approach, this information should be forwarded to the Track/Control process for review, and to determine if the current action plans should be revised.

California Home

Wednesday, November 19, 2003

[HHSDC Home](#)[BP Home Page](#)[The MSC](#)[CMM](#)[POST Enterprise](#)[The Project Office](#)[Life Cycle Processes](#)[Search BP](#)[HHSDC Links](#)[Resources Library](#)[QAWG](#) **NEW!**[SID Policy](#) **NEW!**[Contact Us](#)

search

☒ My CA

Risk Tracking and Control

[Risk Main](#)

Risk Tracking & Control follows the progress of the risk and its exposure, as well as the status of any mitigation and contingency strategies that have been executed.

Periodic re-assessments of the risks should be performed to determine if known risks have become more likely, less likely or have resolved themselves, and to identify new risks as the project progresses.

Some examples of tracking metrics include

- Number of customer requests for changes
- Number of days behind schedule for a particular milestone or deliverable
- Rate of project or vendor staff turnover
- Customer comments on user interface design

The identified metrics and/or events are tracked to determine if there are any changes in the risk profile. In the event the risk exposure increases significantly, the risk should be elevated to project management. Refer to the [SID Policy on Risk Management](#) for a sample risk escalation matrix.

Any mitigation activities should be tracked to determine if they are having the desired effect of reducing risk exposure. If the mitigation strategies do not appear to be having a positive effect, new approaches should be implemented.

The status of significant risks should be discussed at the project management status meetings. The Project Manager may assign additional staff if necessary to assist with additional mitigation activities.

The vendor should report their current high priority risks in their status meetings. The project is also required to report the project risks in status reports to the department.

Samples:

- [Risk Summary Tracking Matrix](#) (MS Excel)
- [Risk Tracking Form](#) (MS Word)

California Home

Wednesday, November 19, 2003

[HHSDC Home](#)[BP Home Page](#)[The MSC](#)[CMM](#)[POST Enterprise](#)[The Project Office](#)[Life Cycle Processes](#)[Search BP](#)[HHSDC Links](#)[Resources Library](#)[QAWG](#) **NEW!**[SID Policy](#) **NEW!**[Contact Us](#) ☒ My CA

Risk Management Communication

[Risk Main](#)

Communication is key to effective risk management. At a minimum, the following types of communications should occur.

- Risk status summary at project management meetings
- Risk information status updates biweekly or monthly
- Periodic risk assessments to identify new risks or significant changes to current risks
- Monthly risk status reports to division management and other stakeholders

California Home

Wednesday, November 19, 2003

[HHSDC Home](#)[BP Home Page](#)[The MSC](#)[CMM](#)[POST Enterprise](#)[The Project Office](#)[Life Cycle Processes](#)[Search BP](#)[HHSDC Links](#)[Resources Library](#)[QAWG](#) **NEW!**[SID Policy](#) **NEW!**[Contact Us](#)

☒ My CA

Risk Management Tool Features

[Risk Main](#)

Typical features of a [risk management system](#) include:

- **Formal Recording-** The risk tracking system must have a mechanism for formally recognizing a risk and recording it for disposition and tracking.
- **Categorization-** The risk tracking system must provide a way to classify and categorize risks to allow for analysis and reporting.
- **Validation-** Not all risks may be worthy of formally recording and expending energy to track. Therefore, the risk tracking system must have a mechanism for review and validation of risks for either closure or action.
- **Probability/Impact Analysis-** The risk tracking system must provide a way to calculate and record the probability of a risk as well as the level of impact if the risk were to occur. Guidelines for performing this analysis and ranking are also needed.
- **Risk Timeframe-** The risk tracking system must capture the expected date the risk will occur.
- **Prioritization-** The risk tracking system must have a mechanism for prioritizing risk. Priority levels should be selected in a manner that maximizes the ability to manage risk and actions to closure.
- **Event Trigger Definitions-** The risk tracking system must capture the event trigger(s) which will cause the contingency plan to be implemented. These triggers should force immediate action.
- **Mitigation Planning-** The risk tracking system must capture and track the mitigation plans, activities and results. In some cases, multiple mitigation plans may be appropriate.
- **Contingency Planning-** The risk tracking system must capture and track the contingency plans, activities and results. In some cases, multiple contingency plans may be appropriate. Each plan may have separate trigger events.
- **Security / Confidentiality-** The risk tracking system must be capable of establishing permissions and maintaining security on a need to know basis. This is particularly important when dealing with procurement or contract risks where compromising of information could lead to legal consequences.
- **Mechanisms For Escalation-** The risk tracking system must provide the ability to escalate risks that have a high impact or probability rating, and risks whose impact/probability has suddenly increased.
- **Risk Tracking / Control-** The risk tracking system must capture status updates and changes in plans or assignment.
- **Reporting-** The risk tracking system must provide the ability to print reports. The exact type and style can be standardized to a great extent. However, the more flexible the reporting feature, the better.
- **Running History Log-** The risk tracking system must track incremental progress notes documented against a risk.

[HHSDC Home](#)[BP Home Page](#)[The MSC](#)[CMM](#)[POST Enterprise](#)[The Project Office](#)[Life Cycle Processes](#)[Search BP](#)[HHSDC Links](#)[Resources Library](#)[QAWG](#) **NEW!**[SID Policy](#) **NEW!**[Contact Us](#)

The purpose of M&O is to continue operational support of the system in production, including periodic maintenance, fixes and changes, until the system is replaced or retired.

☒ My CA

Maintenance and Operations (M&O) Risks

[M&O Main](#)

Some of the common [M&O Pre-Initiation](#) risks include:

- Insufficient or inaccurate documentation and procedures inherited from the development effort
- Insufficient knowledge of the system by the M&O staff
- Insufficient staffing for the M&O phase
- Loss of knowledgeable staff from the development phase
- Insufficient funding to support legislative mandates and changes to user business needs
- Resistance from stakeholders and users if they feel the system does not meet their needs, or if they were inadequately involved in the development process
- Insufficient support or participation from the program sponsor/organization or stakeholders since the system is now developed (they may have other higher priorities now that the system is in M&O)
- Difficulty transitioning from a development mindset to an M&O mindset, particularly if the contractor is continuing in the M&O phase

Other common M&O risks include:

- Tracking versions and releases at the development site and various county sites
- Balancing user needs within the counties to prevent one group from dictating their needs to the whole community
- Balancing user needs with the available funding
- Keeping the program sponsor/organization engaged and involved in policy and system decisions
- Obtaining sufficient funding for technology refreshes, changing user needs, and legislative mandates
- Keeping knowledgeable staff